# Make it and break it - an IoT Smart Home Testbed Case Study

**Abstract**

Education in the information security domain increasingly integrates practical hands-on training; where exercises focusing on secure cyber operations and secure software development are used for training the participants in designing and building secure systems. These exercises utilize multiple approaches in their context, such as capture the flag, attack/defense, reverse engineering, and incident response, while they are conducted on specifically created testbeds that by design integrate vulnerabilities to support the training scenarios. However, these exercises represent only the perspective of the attacker and/or the defender, without reflecting the perspective of the designer, while they statistically have primary focus on network security. In this article, we argue that the best way to understand the consequences of insecure design and development is to combine engineering and exploitation activities in one exercise, proposing the use of "Make it and break it" type of exercises for security training in cyber physical systems. Accordingly, we conducted a case study for validation and verification, the results of which are presented in this article. The case study was performed over the period of two days, during the training boot camp of the Norwegian national team for the European cyber security challenge 2018. During the boot camp, the team has been separated into two groups, which were challenged to design and build an IoT (Internet of Things) smart home using secure design principles, and then attack each other in order to identify security weaknesses. Pre and post-exercise surveys have been conducted, and the feedback from the participants was used in order to evaluate the effectiveness of the exercise, as a pilot towards further development and optimization.